

C-E LCMC Regulation 380-3

Security



Security Classification Guide Procedures

Department of the Army
Headquarters, U.S. Army Communications-Electronics
Life Cycle Management Command (C-E LCMC)
Fort Monmouth, New Jersey
4 January 2006

UNCLASSIFIED

SUMMARY of CHANGE

C-E LCMC Regulation 380-3
Security Classification Guide Procedures

This revision—

- o Clarifies use of “FOUO” term in classification tables (pg. 7).
- o Adds language stressing the importance of citing relevant outside security classification guides (pg. 7, 8).
- o Addresses citation of guidance for Controlled Cryptographic Items (CCI) (pg. 8).
- o Clarifies how to cite outside classification guidance using the specific example of COMSEC (pg. 8, 9).
- o Directs sparing use of “Notes” section, preferring use of “Remarks” column (pg. 8, 17).
- o Corrects format for cover pages (pg. 12).
- o Greatly expands and clarifies how information that may be classified at different levels is handled in the classification tables (pg. 14).
- o Corrects some minor errors and omissions.

Security

Security Classification Guide (SCG) Procedures

Table of Contents

		Paragraph	Page
Chapter 1	Introduction		
	Purpose	1-1	1
	Applicability	1-2	1
	References	1-3	1
	Explanation of Terms	1-4	1
	Background	1-5	2
Chapter 2	SCG Standards		
	Requirement	2-1	3
	Approval	2-2	3
	Reviews	2-3	3
Chapter 3	Preparation Guidelines		
	Related Guidance	3-1	4
	State-of-the-Art Status	3-2	4
	Classification and Declassification	3-3	4
	Derivative Classification	3-4	6
	Foreign Military Sales (FMS) Issues	3-5	6
	General Items	3-6	6
Chapter 4	Writing the SCG		
	Technically Qualified Individuals	4-1	7
	Contractor Personnel	4-2	7
	Statements in SCG	4-3	7
	SCG Structure	4-4	7
	Notes	4-5	8
	References for Derivative Classification	4-6	8

*This Regulation supersedes C-E LCMC Regulation 380-3, 01 Aug 05

Security Classification Guide (SCG) Procedures

Table of Contents – Continued

	Page
Appendixes	
A. C-E LCMC and CERDEC Original Classification Authorities	10
B. Reasons to Classify	11
C. Format for SCG	12
D. Exemptions from Declassification	18
E. Foreign Military Sales (FMS) Issues to be Addressed	19
F. Distribution Statements for Use on Technical Documents	20
G. C-E LCMC DCSINT Local Review Procedures	24

Chapter 1

Introduction

1-1. Purpose

This Regulation—

- a. Provides assistance to project/action officers responsible for writing Security Classification Guides (SCG) for the U.S. Army Communications-Electronics Life Cycle Management Command (C-E LCMC) and other Team C4ISR activities classified projects or programs. See “C-E LCMC DCSINT Local Review Procedures” at Appendix G of this Regulation.
- b. Establishes procedures for eliminating errors in published SCGs.
- c. Specifies information required to produce a uniform format.

1-2. Applicability

This Regulation applies to all C-E LCMC activities and Team C4ISR partners serviced by the C-E LCMC Deputy Chief of Staff for Intelligence (C-E LCMC DCSINT), Fort Monmouth, NJ.

1-3. References

- a. Required reference publications are AR 380-5, 29 Sep 2000, AMC Supplement 1 to AR 380-5, 14 Mar 2003, thereto *Department of the Army Information Security Program*, DoD 5200.1-R, Jan 1997, and the Executive Order (E.O.) 12958, as amended, 25 March 2003.
- b. Other related publications are as follows:
 - DoD 5200.1-I, *Index of Security Classification Guides*.
 - DoD 5220.22.M, *National Industrial Security Program Operating Manual* (NISPOM).
 - AR 360-1, *The Army Public Affairs Program*.
 - DoD Directive 5230.25, *Withholding of Unclassified Technical Data From Public Disclosure*.
 - AR 380-10 and AMC Suppl 1 to AR 380-10, *Foreign Disclosure and Contacts with Foreign Representatives*.
 - AR 25-55, *Freedom of Information Act*.
 - DoD Directive 5230.9, *Clearance of DoD Information for Public Release*.

1-4. Explanation of Terms

For the purpose of this Regulation, the following terms apply:

- a. TOP SECRET – Information or material, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave danger to the national security.
- b. SECRET – Information or material, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.
- c. CONFIDENTIAL – Information or material, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

1-5. Background

Advance classification planning is an essential part of the development of any plan, operation, program, research and development project, or procurement action that involves classified information. A clear, comprehensive SCG is the principal avenue by which a project leader or action officer can ensure adherence to classification determinations. Throughout this Regulation the word “information” refers to knowledge that can be communicated by any means.

In order for information to be submitted to an original classification authority (OCA) in a security classification guide (SCG), the information must be official.

The original classification decision process consists of six steps:

1. Determine that the information is owned by, produced by or for, or is under the control of the U.S. Government.
2. Determine classification eligibility.
3. Decide if unauthorized disclosure would cause damage to national security.
4. Decide the degree of damage and assign a level of classification.
5. Set the duration of classification.
6. Communicate the decision.

Chapter 2

SCG Standards

2-1. Requirement

AR 380-5, paragraph 2-16, requires that a classification guide be issued as soon as practicable before the initial funding or implementation of each classified system, program, project, or plan. AR 380-5, Appendix G, provides guidance for the preparation of SCGs, and Appendix C of this document provides format guidance for SCGs.

2-2. Approval

- a. Each SCG must be personally approved by the original classification authority (OCA) who has been authorized to classify information originally at the highest level of classification prescribed in the SCG.
- b. C-E LCMC and Fort Monmouth approval authorities are listed in Appendix A of this Regulation.

2-3. Reviews

- a. AR 380-5, paragraph 2-19, mandates that SCGs will be reviewed by the originator for currency and accuracy at least once every five (5) years (from the approval date), or if concerning a defense acquisition program, prior to each acquisition program milestone, whichever occurs first.
- b. Timely reviews are critical as classification changes may have occurred during this period, and it is essential that this information be provided to all recipients of the SCGs.
- c. If changes occur to the program before the five (5) year reviews, these changes must be noted and the SCG will be amended or revised. C-E LCMC DCSINT will be notified in writing whenever there is change to the program that requires modification of the SCG.
- d. Upon approval of these changes via C-E LCMC DCSINT staffing, distribution will be made to all recipients of the SCG.
- e. When a program/system is terminated/defielded, C-E LCMC DCSINT will be notified in writing so that the SCG can be removed from the active list of SCGs, per DoD 52001-I.

Chapter 3

Preparation Guidelines

3-1. Related Guidance

a. Guidance may already be in effect covering the information for which you are planning to write an SCG. Therefore, as a prerequisite to starting this task, it is essential that all relevant published guidance be obtained and analyzed. A document or manual will be created for unclassified systems, programs, plans, or projects that will interface with classified systems, programs, plans, or projects. Once these unclassified systems, et al, interact with the classified programs, they will follow the security guidance already in place for these classified programs in their specific SCGs. These guidelines will be outlined in a document or manual that will alert the end user to the fact that when the unclassified system works with the classified one, the security guidance of that classified system will be followed.

b. DoD 5200.1-I, prepared by the Department of Defense (DoD) for this purpose, lists all current DoD SCGs with the exception of those too sensitive to be identified.

3-2. State-of-the-Art Status

a. To ensure that the information considered for classification is placed in proper perspective, it is crucial that you be aware of what has been developed concerning the technology in question, what is being attempted, and by whom. Consider whether the United States has the advantage of technological lead-time.

b. Use scientific and technical information services and consult with technical specialist(s).

3-3. Classification and Declassification

U.S. classification can only be applied to information that is owned by, produced by/for, or is under the control of the US Government. Classification decisions require thoughtful consideration. When information must be classified to protect national security, a simultaneous decision is required as to what level of classification; i.e., Confidential, Secret, or Top Secret (see paragraphs 1-4 above for classification definition). The Presidential E.O. 12958, as amended, dated 25 March 2003, revised classification and declassification procedures, and these must be followed.

a. Classification. The marking "CLASSIFIED BY" is used only for original classification decisions. For those documents that are classified by an original classification authority (OCA), the face of the document will be marked as follows:

CLASSIFIED BY: (followed by the name of personal identifier and position title of the classifier.)

In those situations where it is not otherwise evident, the activity or command and office of origin will be identified and placed below the name on the "CLASSIFIED BY" line. On the next line, the original classifier will identify the reason(s) (outlined in the Executive Order) for the decision to classify. The "REASON" for classification relates to the categories of what can be classified as specified in Section 1.4 (a-h) of the Executive Order, as amended. Reasons to determine what can be classified are listed in Appendix B of this Regulation. Codes will be used in the preparation of all SCGs (see Appendix C for the insertion location for the "REASON" codes).

For Original Classification Decisions: No 25X marking, other than "25X1-human," is permitted on the "Declassify on" line when an original classification decision is made. There are no exceptions to this policy. According to the guidance from the Information Security Oversight Office (ISOO):

The marking applied to information exempted from the 25-year automatic declassification provisions of EO 12958, as amended, cannot be used until the exemption is approved through the ISCAP (International Security Classification Appeals Panel) process or permitted by the Panel's Executive Secretary.

- (1) When determining the duration of classification in the first instance, i.e., original classification, the original classification authority has four choices: (i) a date or event less than 10 years from the date of the decision;

- or (ii) a date 10 years from the date of the decision; or (iii) a date greater than 10 years and less than 25 years from the date of the decision; or (iv) a date 25 years from the date of the decision.
- (2) The only exception to the four choices identified above is the marking “25X1-human.” This marking may be used when the disclosure of the information could be expected to reveal the identity of a confidential human source or human intelligence source. “25X1-human” is the *only* 25X marking that does not require a date or event for declassification to be cited with the 25X marking.
 - (3) Information that could be expected to reveal information about the application of an intelligence source or method, though a part of 25X1, is separate and distinct from the marking, “25X1-human.” Agencies may not use the marking “25X1-human” for non-human intelligence sources or for intelligence methods.

b. Declassification.

- (1) A declassification determination is as significant as the original decision. Therefore, when original classification decisions are made, a conclusion must be reached concerning how long classification is required, i.e., duration of time, specific date or event.
- (2) The last line of the classification authority and declassification instruction will be “DECLASSIFY ON” instruction. The original classifier shall attempt to establish a specific date or event for declassification based upon the national security sensitivity of the information, or an exemption category. The term “OADR” or “originating agency’s determination required” is no longer authorized for use. When a specific date or event is used, there is no change from existing policy stated in AR 380-5 and E.O. 12958, as amended.
- (3) Subject to paragraphs (b-e), E.O. 12958, as amended, Section 3.3, paragraph (a), “...on December 31, 2006, all classified records that (1) are more than 25 years old, and (2) have been determined to have permanent historical value under Title 44, US Code, shall be automatically declassified whether these records have been reviewed or not. Subsequently, all classified records shall be automatically declassified on December 31 of the year that is 25 years from the original classification date.”
- (4) When a specific date or event within 25 years cannot be established because the information is exempt, the original classifier will apply the letter “X” plus a brief recitation of the exemption category(ies) in section 3.3 (b) of the Executive Order, i.e., 25X4 – “reveal information that would impair the application of state-of-the-art technology within a U.S. weapon system”. The 25X markings are the only authorized markings for the identification of information approved by the President or the ISCAP for classification beyond 25 years, but approval must be obtained in order to use these. The 25X markings shall not be used for any other classified information. This information will remain classified until reviewed again. Exemption categories and codes are listed in Appendix D.

c. Downgrading.

- (1) When your effort is originally conceived, you may feel that it is important to classify information that you are aware will lose some sensitivity as development progresses.
- (2) Your SCG will specify details for downgrading this information to a lower level of classification when the lower level will provide adequate protection.

3-4. Derivative Classification

a. Most Army classified documents are derivatively classified in that the classification is based upon a classification guide or source document(s) already in existence. If an SCG references all derivative sources for its classification, then that SCG is not a candidate for Original Classification Authority (OCA). For derivative classification decisions, the term “DERIVED FROM” will replace the term “CLASSIFIED BY.” There is no requirement to include a “REASON” line. The “DECLASSIFY ON” line must be determined by the appropriate original classification authority. The derivative classification will indicate the source document or the classification guide on the “DERIVED FROM” line, including the agency, activity, or command and office of origin, and the date of the source or guide. When a document is classified derivatively on the basis of more than one source document or classification guide, the “DERIVED FROM” line will read “MULTIPLE SOURCES” and the derivative classifier will keep a list of sources with the file or record copy of the derivatively classified document.

b. When a specific date or event is listed on the source document or declassification guide, the derivatively classified document will show the date or event after the term “DECLASSIFY ON.” Many current source documents and classification guides indicate the term “OADR” or “Originating Agency’s Determination Required” as declassification instruction. Until classification guides are rewritten and unless otherwise instructed by the original classifier, the derivative classifier will carry forward the fact that the source was marked a “OADR,” and the date of origin of the most recent source document, classification guide, or specific information being classified; for example:

DERIVED FROM:	C-E LCMC Memo “Classification Marking”
DECLASSIFY ON:	Source Marked “OADR,” 20041130

3-5. Foreign Military Sales (FMS) Issues

An important aspect of all SCGs is FMS issues. Specific data elements required to facilitate FMS deliberation must be included in the “Foreign Government Information and Foreign Military Sales” section (1-7) of each SCG. For a template of Section 1, see Appendix C. See Appendix E of this regulation for FMS issues to be addressed.

3-6. General Items

The following generic points are to be considered when SCGs are developed:

- a. Explanation of initial operational capability (IOC) as to whether it is a specific date (year, month, and day) or an event; e.g., upon fielding of a specific weapon system. Also, to protect an IOC date, define the size of the “window” which will be used instead of a specific date.
- b. If a “first unit equipped” is listed as classified by an SCG, to what size unit does it pertain (company, battalion, etc.)?
- c. Identify the specific point during the test phase of an item when test date becomes classified; e.g., when test data for 10 years or more tests is summarized.
- d. All SCGs will be written specifically to the system/program they pertain to rather than generalizations.

Chapter 4

Writing the SCG

4-1. Technically Qualified Individuals

While various individuals may provide input to an SCG, someone who is technically qualified and has total knowledge of the system, program, plan, or project will write the SCG.

4-2. Contractor Personnel

When the contractors who will be working on a particular project have been identified, solicit their assistance in writing the SCG, but the Action Officer for each SCG will be from the activity's government staff. The contractors' expertise and knowledge of the various facets of the system can be extremely beneficial in producing a workable SCG for all users.

4-3. Statements in the SCG

- a. An SCG precisely states the specific items or elements to be protected. There must be no uncertainty as to the intent. Never write in a manner that permits the user to make "de facto" original classification decisions.
- b. Clear, concise statements will be provided covering levels of classification for documentation and program components involved in every phase of the effort.
- c. When an item must show a range of classifications, clearly define the criteria for assigning each level of classification. Ensure that you provide an adequate explanation as to when the item is unclassified and when it is classified.

4-4. SCG Structure

See Appendix C for security SCG format. For those Sections that require the use of a table, use the following format. (See Appendix C for Examples of the table structure.)

- a. The body of the SCG will be divided into columns as follows:
 - (1) COLUMN 1 – Identify the item or element of information involved. If the preparer desires, this column may be headed "Item" or "Element," but does not require a heading.
 - (2) COLUMN 2 – This column is headed "Level," and will indicate classification of item; e.g., "TS," "S," "C," or "U." The term "FOUO" (For Official Use Only) or similar markings will not be used in this column, as they are not levels of classification. If unclassified items need to be treated as FOUO, make sure to explain this in the "Remarks" column.
 - (3) COLUMN 3 – This column is headed "Reason" and will indicate the reason for classification. See Chapter 3 and Appendix B for further guidance.
 - (4) COLUMN 4 – This column is headed "Duration," and will indicate a date or event. If the date is cited in a number form, use the YYYYMMDD format. See Chapter 3 and Appendix D for further guidance.
 - (5) COLUMN 5 – This column is headed "Remarks."
 - (a) If needed, insert a brief statement clarifying the classification decision. If more detail is needed than can practically fit in the column, insert "See Note #" and provide an explanation in the "Notes" portion of the SCG.
 - (b) If classification falls under the purview of another agency, i.e., COMSEC items under NSA guidance, please provide a citation of the NSA guidance for the specific item in the Section 1 of the SCG. If it is

important to the SCG preparer that NSA guidance be reiterated in the SCG, that guidance will be expressed in the classification tables with all other important items—along with citations of the guidance in the “Remarks” column. If an item has no available guidance, provide a concurrence memo from the outside agency (in this case, NSA) indicating they are aware of the responsibility to provide guidance. This will also apply to items under DIA or any other agency’s or military service’s authority.

(c) Show special access designations or dissemination, and who is responsible for these.

(d) Indicate special downgrading/duration instructions, if any.

4-5. Notes

The addition of a “Notes” section to an SCG is possible, but discouraged. Special instructions and remarks should be placed in the “Remarks” column. Notes may be added to the end of the SCG as the last section—*only* if the amount of text needed for remarks becomes too great to practically fit in the “Remarks” column. All original classification decisions will be reflected in the tables. Therefore, notes at the end of an SCG must *never* contain additional instructions that affect the classification of an item unless those instructions are reflected in the table. Notes will be referenced in the “Remarks” column by stating, “See Note #.”

4-6. References for Derivative Classification

Often, information or components used in a system are already classified by another SCG. It is critically important that an OCA does not re-classify information that has already been classified. This could be especially dangerous if information is re-classified at a different level or for a different duration.

It is up to the preparer of an SCG to make certain that all authoritative SCGs (or other documents) are cited when items in an SCG are classified derivatively. These citations will be placed in the “Remarks” column of the related item if possible. If, instead, the SCG includes the citations as part of a larger list, make sure to put an appropriate reference in the “Remarks” column directing the user to that list.

The citation of guidance from outside agencies or military branches often presents a special problem for SCG preparers. This often occurs particularly with COMSEC guidance under the authority of NSA. The classification guidance for many COMSEC devices can be found within documents cited in the Committee on National Security Systems (CNSS) Index of National Security Systems Issuances. This index can be found at <http://www.cnss.gov>. It is also important to note that the overarching NSA guidance—NTISSI (National Telecommunications and Information System Security Instruction) 4002, Classification Guide for COMSEC Information, dated 05 June 1986, is not authorized for distribution to Army users. Instead, guidance from NTISSI 4002 has been incorporated into the AR 380-40, Policy for Safeguarding and Controlling Communications Security (COMSEC) Material, dated 30 June 2000, Appendix B. NSA, however, remains the proponent for COMSEC guidance, so the AR 380-40 must not be cited as the original source for such guidance. The SCG preparer should assist the end user of the SCG by first calling attention to the guidance provided by the AR 380-40, then citing NTISSI 4002 as the original source.

In some instances, a system may contain a Controlled Cryptographic Item (CCI). In this case, the DA Pamphlet 25-380-2, Security Procedures for Controlled Cryptographic Items, dated 10 Jan 1991, should be cited as classification guidance for these particular items.

EXAMPLE:

A Widget-9 system utilizing KIV-7 and KG-66 COMSEC devices needs an SCG.

Scenario 1: The preparer may simply include a section on COMSEC within Section 1 of the SCG. The following statement would be appropriate:

The Widget-9 system utilizes KG-66 and KIV-7 COMSEC devices. NSA has classification authority for COMSEC material. COMSEC material in the Widget-9 system will be classified and handled in accordance with: NSTISSI 3017, Operational Security Doctrine for Non-TRI-TAC KG-84A, KG-84C, KIV-7, and KIV-7HS, KIV-7HSA, and KIV-7HSB, dated March 2003, NSTISSI 3003, Operational Security Doctrine for the KG-66/KG-66A/SO-66/KGR-66/KGV-

68/KGR-68/KGV-68B, dated August 2000, and NTISSI 4002, Classification Guide for COMSEC information, dated 05 June 1986. For Army users, guidance from NTISSI 4002 can be found in AR 380-40, Policy for Safeguarding and Controlling Communications Security (COMSEC) Material, dated 30 June 2000, Appendix B.

Scenario 2: The SCG preparer feels the need to reiterate classification guidance for the COMSEC material in the system SCG. In addition to citing overarching NSA guidance in Section 1, such as NTISSI 4002, the preparer will place specific COMSEC items in the classification tables, and then provide the appropriate guidance in the following manner:

	Level	Reason	Duration	Remarks
1. KIV-7	-----	(as directed by NSA guide)	-----	Guidance derived from NSTISSI 3017, Operational Security Doctrine for Non-TRI-TAC KG-84A, KG-84C, KIV-7, and KIV-7HS, KIV-7HSA, and KIV-7HSB, dated March 2003.
2. KG-66	-----	(as directed by NSA guide)	-----	Guidance derived from NSTISSI 3003, Operational Security Doctrine for the KG-66/KG-66A/SO-66/KGR-66/KGV-68/KGR-68/KGV-68B, dated August 2000.

An SCG preparer must remain mindful, however, that an SCG should be an unclassified document if possible. Due to the fact that some guidance for COMSEC material is classified, the option laid out in Scenario 1 may be even more preferable.

While the examples above deal with COMSEC, this approach will be used to cite guidance from any outside agency or military branch.

Appendix A

C-E LCMC and CERDEC Original Classification Authorities

For the C-E LCMC:

Position

Level of OCA

Commanding General and Program Executive Officer,
Command Control and Communications Tactical

Up to TOP SECRET

Program Executive Officer,
Command, Control and Communications Tactical

Up to SECRET

Chief of Staff,
U.S. Army Communications-Electronics
Life Cycle Management Command

Up to SECRET

For the CERDEC:

Position

Level of OCA

*Director, US Army Communications Electronics
Research, Development, and Engineering Center

Up to SECRET

*OCA up to the TOP SECRET level resides with the Commander, RDECOM.

Appendix B

Reasons to Classify

The below listed categories of what can be classified as specified by Executive Order 12958, as amended, Section 1-4 (a-h), will be used for the “Reason” when classifying components of the SCG:

- a. Military Plans, weapons systems, or operations.
- b. Foreign government information.
- c. Intelligence activities (including special activities), intelligence sources or methods, or cryptology.
- d. Foreign relations or foreign activities of the United States, including confidential sources.
- e. Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism.
- f. United States Government programs for safeguarding nuclear materials or facilities.
- g. Vulnerabilities or capabilities of systems, installations, infrastructures, projects, or protection services relating to the National Security, which includes defense against transnational terrorism.
- h. Weapons of mass destruction.

Appendix C

Format for SCG

Each SCG will have a cover page that will contain the overall classification of the SCG, the symbol of Team C4ISR/New Jersey, the symbol of the responsible activity (if possible), the name of the SCG, and the correct Distribution Statement (See Appendix F).

The SCG will be formatted in landscape style. If the SCG is For Official Use Only (FOUO), this caveat will be annotated on the bottom of each page in 14 point font and on the back page. A Table of Contents (TOC) will be included in each SCG and will follow the Approval Page.

The second page of the SCG is the Approval page and will be formatted as follows:

Issued By: *(Insert name and address of activity responsible for SCG.)*

Approved By: *(Insert correct title of applicable OCA and affiliation.)*

Date: *(Leave blank. This is the date of approval, and will be filled in by C-E LCMC DCSINT, after OCA approval.)*

Program Numbers: *(Insert # or, if none, so state.)*

Supersession(s): *(Insert name and date of previous SCG. If new SCG, so state.)*

Action Officer: *(Insert name, address, commercial telephone number, DSN telephone number.)*

Distribution Statement: *(Insert appropriate distribution statement for SCG program. See Appendix F.)*

Appendix C – Continued

Section 1 – General Information

1. Purpose: To provide instructions and guidance on the security classification of information and material pertaining to *(title of project)*.
2. Authority: This SCG is issued under the authority of AR 380-5, 29 Sep 2000, AMC Supplement 1 to AR 380-5, 14 Mar 2003, E.O. 12958, as amended, 25 Mar 2003, and DoD 5200.1-R, *Information Security Program*, Jan 1997. It constitutes authority and may be cited as the basis for classification, regrading, or declassification of information concerning *(title of project)*. Unless otherwise noted, the authority of the approving official on the title page classifies information or material identified as classified in this SCG.
3. Application: Changes in classification required by this SCG will be made immediately and reported in writing by the Office of Primary Responsibility (OPR) to C-E LCMC DCSINT, AMSEL-MI, Ft. Monmouth, NJ 07703-5003 for processing and dissemination.
4. Questions and Recommendations: Questions concerning the content and interpretation of this SCG will be directed to the issuing activity. If the security classification imposed by this SCG is considered impractical, documented and justified recommendations will be made through appropriate channels to the issuing activity. If current conditions, progress made in this effort, scientific or technological developments, advances in the state-of-the-art, or other factors indicate a need for changes, similar recommendations will be made. Pending a final decision, the information involved will be protected at either the currently specified level or the recommended level, whichever is higher. All users of this SCG are encouraged to assist in improving its currency and adequacy. Any over-classification or incorrect classification will be brought to the attention of the issuing activity, who will report these changes in writing to C-E LCMC DCSINT.
5. Public Release: The fact that certain details of information are shown to be unclassified does not authorize automatic public release. Proposed public releases of unclassified information must be processed through appropriate channels for approval for publication. Within the Department of the Army, the procedures specified in AR 360-1 will be followed. Defense contractors will comply with DoD 5220.22-M (NISPOM) and other contractual requirements. All information concerning (name of project/SCG) will be forwarded for public release to Commander, C-E LCMC, ATTN: AMSEL-IO, Fort Monmouth, New Jersey 07703-5000, in accordance with AR 360-1, paragraph 5-3. For guides not under the purview of C-E LCMC, use the command procedures for public release.
6. Definitions: *(Terms unique to subject SCG—if none state “None”)*
7. Foreign Government Information and Foreign Military Sales: *(Include here when necessary, any data to provide guidance on marking and protecting foreign government information pertinent to project or to make reference to the Security Assistance Management Manual. Appendix E lists the items to be addressed on foreign military sales.)*
8. Foreign Disclosure: Any disclosure to foreign officials of information classified by this SCG shall be in accordance with the procedures set forth in AR 380-10 and NDP-1. If a country with which the Department of Defense has entered into a reciprocal procurement memorandum of understanding or offset arrangement expresses an interest in this effort, a foreign disclosure review will be conducted prior to issuance of a solicitation. If it is known that foreign participation cannot be permitted because of the sensitivity of the effort, this fact will be stated.
9. Description: Provide a brief unclassified description of the system, program, plan, or project.

Appendix C – Continued

Important note: One of the most troublesome aspects of creating an SCG is dealing with elements of a system that are classified at different levels depending on certain circumstances—this includes issues of compilation.

Previously, this problem was typically dealt with in tables by expressing the range of possible classifications in the level column. A range of levels might have been shown as “U, C, S,” or “U-S”. This notation, however, could be confusing for some. For example, “U, S” has a different meaning than “U-S” (“U-S” includes “C”, whereas “U, S” does not). Additionally, many SCG preparers were concerned that the end user would be too likely to mistakenly under (or over) classify an item without spending the time to adequately read instructions in remarks or notes.

From this point forward, circumstances that dictate a range of possible classifications for an item will, if practicable, be delineated in the first (“Item” or “Element”) column.

EXAMPLE:

This style:

	Level	Reason	Duration	Remarks
1. Widget broadcast range	U, C, S	1.4a, g	20151130	UNCLASSIFIED when describing range in LARRY Band. CONFIDENTIAL when describing range in the MOE or CURLY Band. By compilation, SECRET when ranges in MOE and CURLY Bands are described together.

Will be replaced with this style:

	Level	Reason	Duration	Remarks
1. Widget broadcast range				
a. In LARRY Band	U	1.4a, g	20151130	
b. In MOE or CURLY Band	C	1.4a, g	20151130	
c. By compilation, when ranges in MOE and CURLY Bands are described together	S	1.4a, g	20151130	

The new format leaves no question as to the level the item will be classified at, and for how long. There is also no chance that the end user will ignore specific instructions in the “Remarks” column, because there are none. In this example, the need for any special instruction in the “Remarks” column is eliminated completely.

Notations like “U, C, S” or “U-S” in the “Level” column may be used in rare instances, but only if an item’s classification cannot be delineated in the first column, and a more narrative explanation is required in the “Remarks.”

Section 2 – Overall Effort

Use this section to identify the effort, the goal, mission, military application, end item, etc. State the level of classification for each item or if that end item is unclassified.

EXAMPLE:

	Level	Reason	Duration	Remarks
1. Nomenclature	U			
2. Goal, mission, purpose	U			
3. Military application	C	1.4a	20151130	Could reveal info on military plans
4. End item				
a. External View	U			
b. Internal View	C	1.4c	20151120	Could reveal cryptology

Section 3 – Performance and Capabilities

List each detail of information that identifies the characteristics of performance and capability of an end item or its component, part, or material. State the level of classification for each item or that it is unclassified.

	Level	Reason	Duration	Remarks
EXAMPLE:				
1. Range				
a. Actual	S	1.4a	20151130	Could reveal military operation
b. Planned	U			
2. Speed				
a. Maximum	S	1.4g	20151130	Could reveal system capability
b. Intercept	S	1.4g	20251130	Could reveal system capability

Appendix C – Continued

Section 4 – Specifications

Precisely state specifications concerning this effort that warrant classification or are unclassified. This section will address the characteristics of the system.

EXAMPLE:

	Level	Reason	Duration	Remarks
1. Size	U			
2. Weight	U			
3. Power Requirement	U			

Section 5 – Critical Elements

List items that are peculiar to this effort and which must be classified. If they are included in other sections of the SCG, merely state “Not Applicable” in this section. For further guidance, see AR 380-5, Appendix G, Section V.16.

Section 6 – Vulnerabilities and Weaknesses

State any deficiencies that could make this effort vulnerable to failure. Include classification for countermeasures and counter-countermeasures.

EXAMPLE:

	Level	Reason	Duration	Remarks
1. Operational Countermeasures				
a. Techniques involved	C	1.4g	20151130	Could reveal system weakness
b. Effects of countermeasures	S	1.4g	20151130	Could reveal system weakness
2. Electromagnetic Pulse	S	1.4c,g	20251130	Could reveal cryptology, system capability

Appendix C – Continued

Section 7 – Administrative Data

Provide detailed information concerning research and development program, procurement and production, milestones, tactical deployment, etc. Indicate the level of classification for each item or, if unclassified, state that fact.

EXAMPLE:

	Level	Reason	Duration	Remarks
1. Research and Development Funds				
a. Budget year(s), execution year and prior year(s)	U			
b. Future year(s)	U			
2. Schedule				
a. Initial Operating Capability (IOC)	U			
b. Fielding Schedule	U			
3. Procurement/Production Program				
a. Quantities (world-wide assets)	U			
b. Funds (Budget year[s], execution year, and prior year[s])	U			

Section 8 – Hardware and Software

If the effort involves using electronic data processing equipment, the classification of software/hardware must be included.

Section 9 – Notes

The addition of a “Notes” section to an SCG is possible, but discouraged. Special instructions and remarks will be placed in the “Remarks” column. Notes may be added to the end of the SCG as the last section—*only* if the amount of text needed for remarks becomes too great to practically fit in the “Remarks” column. All original classification decisions will be reflected in the tables. Therefore, notes at the end of an SCG must *never* contain additional instructions that affect the classification of an item unless those instructions are reflected in the table. Notes will be referenced in the “Remarks” column by stating, “See Note #.”

Appendix D

Exemptions from Declassification

The below listed categories of EXEMPTIONS will be used when a specific date or event cannot be established to declassify documents, as specified in Executive Order 12958, as amended, Section 3.3b, 25 March, 2003. According to the guidance from ISOO, the marking applied to information exempted from the 25-year automatic declassification provisions of E.O. 12958, as amended, cannot be used until the exemption is approved through the ISCAP process or permitted by the Panel's Executive Secretary.

25X-1 – Reveal the identity of a confidential human source, or a human intelligence source (should be marked as follows, 25X1-human), or reveal information about the application of an intelligence source or method and is not subject to automatic declassification. *This is the only 25X marking permitted on the "Declassify on" line when an original classification decision is made that does not require a date or event for declassification to be cited. There are no exceptions to this policy.*

25X-2 – Reveal information that would assist in the development or use of weapons of mass destruction;

25X-3 – Reveal information that would impair U.S. cryptologic systems or activities;

25X-4 – Reveal information that would impair the application of state-of-the-art technology within a system;

25X-5 – Reveal actual U.S. military war plans that remain in effect;

25X-6 – Reveal information, including foreign government information, that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;

25X-7 – Reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of the national security, are authorized;

25X-8 – Reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security;

25X-9 – Violate a statute, treaty, or international agreement.

Appendix E

Foreign Military Sales (FMS) Issues to be Addressed

If applicable, address these FMS issues in Section 1, paragraph 7 of the SCG, “Foreign Government Information and Foreign Military Sales”:

- * Highest level of classified information that is necessarily disclosed by sale of end item.
- * Highest level of classified information that is necessarily disclosed to enable production of end item.
- * Highest level of classified information that is necessarily disclosed to allow maintenance of the end item.
- * Highest level of classified information that is necessarily disclosed in training to use the end item.
- * Highest level of information that could be revealed by reverse engineering of the end item.
- * Highest classification of information that could be revealed by testing the end item.

Appendix F

Distribution Statements for Use on Technical Documents

The following distribution statements are authorized for use on DoD technical documents.

1. **DISTRIBUTION STATEMENT A.** Approved for public release; distribution is unlimited.

- a. This statement may be used only on unclassified technical documents that have been cleared for public release by competent authority in accordance with DoD Directive 5230.9. Technical documents resulting from contracted fundamental research efforts will normally be assigned distribution statement A, except for those rare and exceptional circumstances where there is a likelihood of disclosing performance characteristics of military systems or if manufacturing technologies that are unique and critical to defense, and agreement on this situation has been recorded in the contract or grant.
- b. Technical documents with this statement may be made available or sold to the public and foreign nationals, companies, and governments, including adversary governments, and may be exported.
- c. This statement may not be used on technical documents that formerly were classified unless such documents are cleared for public release.
- d. This statement shall not be used on classified technical documents containing export controlled technical data as provided in DoD Directive 5230-25.

2. **DISTRIBUTION STATEMENT B.** Distribution authorized to U.S. Government agencies only (fill in reason). Date of determination is the approval date of this document or date of earlier approved SCG, if current SCG is a revision. Other requests for this document shall be referred to (insert controlling DoD office/activity).

- a. This statement may be used on unclassified and classified documents.
- b. Reasons for assigning distribution statement B include –

Foreign Government Information	To protect and distribution in accordance with the desires of the foreign government that furnished the technical information. Information of this type normally is classified at the CONFIDENTIAL level or higher.
Proprietary Information	To protect information not owned by the U.S. Government and protected by a contractor's "limited rights" statement or received with the understanding that it not be routinely transmitted outside the U.S. Government.
Critical Technology	To protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary. Information of this type may be classified or unclassified; when classified, it is export-controlled and subject to the provisions of DoD Directive 5230-25.
Test and Evaluation	To protect results of tests and evaluation of commercial products of military hardware when such disclosure may cause unfair advantage or disadvantage to the manufacturer of the product.
Contractor Performance	To protect information in management reviews, records of contract performance evaluation, or other advisory documents evaluating programs of contractors.

Appendix F – Continued

Premature Dissemination	To protect patentable information on systems or processes in the development or concept stage from premature dissemination.
Administrative or Operational Use	To protect technical or operational data or information from automatic dissemination under the International Exchange Program or by other means. This protection covers publication required solely for official use or strictly for administrative or operational purposes. This statement may be applied to manuals, Regulations, technical orders, technical reports, and other publications containing valuable technical or operational data.
Software Documentation	Releasable only in accordance with DoD Instruction 7930.2.
Specific Authority	To protect information not specifically included in the above reasons and discussions but which requires protection in accordance with valid documented authority such as Executive Orders, classification SCGs, DoD, or DoD component regulatory documents. When filling in the reason, cite “Specific Authority (identification of valid documented authority).”

3. DISTRIBUTION STATEMENT C. Distribution authorized to U.S. Government agencies and their contractors (fill in reason) and date of determination is the approval date of this document or date of earlier approved SCG, if current SCG is a revision. Other requests for this document shall be referred to (insert controlling DoD office/activity).

a. Distribution statement C may be used on unclassified and classified technical documents.

b. Reasons for assigning distribution statement C include –

Foreign Government	Same as distribution statement B.
Critical Technology	Same as distribution statement B.
Software Documentation	Same as distribution statement B.
Administrative or Operational Use	Same as distribution statement B.
Specific Authority	Same as distribution statement B.

4. DISTRIBUTION STATEMENT D. Distribution authorized to the Department of Defense and U.S. DoD contractors only (fill in reason) and date of determination is the approval date of this document or date of earlier approved SCG, if current SCG is a revision. Other requests for this document shall be referred to (insert controlling DoD office/activity).

a. Distribution statement D may be used on unclassified and classified technical documents.

b. Reasons for assigning distribution statement D include –

Foreign Government Information	Same as distribution statement B.
Administrative or Operational Use	Same as distribution statement B.

Appendix F – Continued

Software Documentation	Same as distribution statement B.
Critical Technology	Same as distribution statement B.
Specific Authority	Same as distribution statement B.

5. DISTRIBUTION STATEMENT E. Distribution authorized to DoD components only (fill in reason), and date of determination is the approval date of this document or date of earlier approved SCG, if current SCG is a revision. Other requests shall be referred to (insert controlling DoD office/activity).

- a. Distribution statement E may be used on unclassified and classified technical documents.
- b. Reasons for assigning distribution statement E include –

Direct Military Support	This document contains export-controlled technical data of such military significance that release for purposes other than direct support of DoD approved activities may jeopardize an important technological or operational military advantage of the United States. Designation of such data is made by competent authority in accordance with DoD Directive 5230-25.
Foreign Government Information	Same as distribution statement B.
Proprietary Information	Same as distribution statement B.
Premature Dissemination	Same as distribution statement B.
Test and Evaluation	Same as distribution statement B.
Software Documentation	Same as distribution statement B.
Contractor Performance Evaluation	Same as distribution statement B.
Critical Technology	Same as distribution statement B.
Administrative or Operational Use	Same as distribution statement B.
Specific Authority	Same as distribution statement B.

6. DISTRIBUTION STATEMENT F. Further dissemination only as directed by (insert controlling DoD office/activity), and date of determination is effective approval date of this document or date of earlier approved SCG, if current SCG is a revision or higher DoD authority.

- a. Distribution statement F is normally used only on classified technical documents, but may be used on unclassified technical documents when specific authority exists (e.g., designation as direct military support as in statement E).

Appendix F – Continued

b. Distribution statement F is also used when the DoD originator determines that information is subject to special dissemination limitation.

7. **DISTRIBUTION STATEMENT X.** Distribution authorized to U.S. Government agencies and private individuals or enterprises that are eligible to obtain export-controlled technical data in accordance with DoD 5230.25 (date of determination is effective approval date of this document). Controlling DoD office/activity is (insert).

a. Distribution statement X shall be used on unclassified documents when distribution statements B, C, D, E, or F do not apply, but the document does contain technical data as explained in DoD 5230.25.

b. This statement shall not be used on classified technical documents, however, it may be assigned to technical documents that formerly were classified.

8. **EXPORT CONTROL WARNING.** All technical documents that are determined to contain export-controlled technical data shall be marked –

“WARNING – This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22 U.S.C., Sec 275, et seq) or the Export Administration Act of 1979, as amended, Title 50, U.S.C. App 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provision of DoD Directive 5230.25.”

When it is not technically feasible to use the entire statement, an abbreviated marking may be used with a copy of the full statement added to the “Notice to Accompany Release of Export Controlled Data” required by DoD Directive 5230.25.

9. **HANDLING AND DESTROYING UNCLASSIFIED/LIMITED DISTRIBUTION DOCUMENTS.**

Unclassified/Limited Distribution documents shall be handled using the same standards for “For Official Use Only (FOUO)” material, and will be destroyed by any method that will prevent disclosure of contents or reconstruction of the document. When local circumstances or experience indicates that this destruction method is not sufficiently protective of unclassified limited information, local authorities may prescribe other methods but must give due consideration to the additional expense balance against the degree of sensitivity.

Appendix G

C-E LCMC DCSINT Local Review Procedures

- Action Officer (AO) contacts C-E LCMC DCSINT Security Specialist.
- How information will be identified for protection and covered in a SCG is discussed between AO and C-E LCMC DCSINT Specialist.
- Information must fall under purview of approved OCA: CG (TS); CS (S); PEO C3T (S); or Director CERDEC (S).
- SCG reviewed by C-E LCMC DCSINT specialist for soundness of classification decisions.
- Challenges are discussed with AO and coordinated as needed.
- Final SCG (electronic version) with concurrence memo from center's director/activity head are submitted to C-E LCMC DCSINT to staff and process for OCA approval.
- OCA returns SCG with approval, and C-E LCMC DCSINT distributes IAW AMC Supplement 1 to AR 380-5, 14 Mar 2003.
- C-E LCMC DCSINT sends electronic version with approval date back to the activity POC as well as hard copies of SCG and related correspondence.
- C-E LCMC DCSINT will update current SCG List and post on the C-E LCMC DCSINT Splash Page on the Team C4ISR Knowledge Center.

The proponent of this publication is the U.S. Army Communications-Electronics Life Cycle Management Command, Fort Monmouth, NJ. Users are invited to send comments on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to U.S. Army, C-E LCMC DCSINT, Attn: AMSEL-MI, Fort Monmouth, NJ 07703-5003.

OFFICIAL:

MICHAEL R. MAZZUCCHI
Major General, USA
Commanding and PEO

A handwritten signature in black ink, appearing to read 'Kent Woods', is written over a large, faint circular stamp.

KENT T. WOODS
Colonel, GS
Chief of Staff